مكافحة
الرقابة الإلكترونية

HRDO
هردو

مركز هردو
لدعم التعبير الرقمي
HRDO CENTER
To Support the Digital Expression

مكافحة
الرقابة الإلكترونية

مركز هردو لدعم التعبير الرقمي
القاهرة ٢٠١٦

مكافحة الرقابة الالكترونية

مركز هردو

لدعم التعبير الرقمي

www.hrdoegypt.org

info@hrdoegypt.org

المحتويات

اليوم العالمي لمكافحة الرقابة الإلكترونية

اليوم العالمي لمكافحة الرقابة الإلكترونية والذي يصادف الثاني عشر من شهر مارس كل عام، عقد للمرة الأولى في ١٢ مارس ٢٠٠٨ بناءً على طلب من منظمة مراسلون بلا حدود ومنظمة العفو الدولية.

حيث كان قد أرسل خطاب كتبه كل من "جان فرانسوا جوليار"، الأمين العام لمنظمة مراسلون بلا حدود، و"لاري كوكس" المدير التنفيذي لمنظمة العفو الدولية، إلى كبار المسؤولين التنفيذيين في جوجل، وياهو، وإنك، وشركة مايكروسوفت لطلب مراقبة اليوم.

والهدف الأساسي من هذا اليوم هو التوعية من المخاطر التي تهدد حرية الإنترنت من مراقبة وتعقب للمستخدمين وحجب للمواقع، والى دعم شبكة إنترنت تضمن حرية التعبير عن الرأي بعيدا عن التدابير التي تنتهجها بعض الحكومات لإسكات الاصوات على الشبكة.

وبمناسبة هذا اليوم يقدم مركز هردو ورقته التعريفية بهذا اليوم ويناقش أهم النقاط الرئيسية حول الرقابة الإلكترونية والتوعية بخطر تلك المسألة.

يعني إيه رقابة إلكترونية؟

الرقابة على الإنترنت معناها التحكم في نشر والوصول إلى المعلومات على الإنترنت، وتستخدم في الرقابة تقنية تعتمد على جدار ناري أو بروكسي، ويتم ذلك من خلال إجبار جميع المتعاملين مع الشبكة على المرور عبر خوادم البروكسي قبل الوصول إلى الشبكة.

وتقوم الحكومات ومزودو خدمة الانترنت في العديد من دول الشرق الأوسط بحجب مواقع تحتوي على معلومات لا يتفقون معها، إما لأنّ السلطات لا تسمح بانتشار وجهة نظر الموقع المحجوب أو ببساطة لأن الصفحة المحجوبة تحتوي على كلمات من قائمة الكلمات المحظورة لدى هذه السلطات. كما هو الحال على سبيل المثال، مع المواقع التي تحتوي على كلمة "إسرائيل"، والتي تعتبر من المواقع الأكثر حجباً في الشرق الأوسط.

وهناك نوعان رئيسيان من الرقابة:

أولهما الرقابة النشطة وهي التي تقوم فيها السلطات بالتدخل فعلياً لمنع وصول منشورات معينة إلى الناس. ويحتاج هذا النوع من الرقابة إلى الاستعانة بأدوات تقنية وماسحات ومراقبين يتابعون ما تنشره مواقع الانترنت.

والنوع الآخر هو الرقابة الذاتية. ولعل هذا النوع من الرقابة هو الأكثر إشكالية لأن نجاحه يعتمد على خوف القائمين على المواقع من إغضاب السلطات فيمتنعون عن نشر مواد إشكالية لتجنب المواجهات القانونية، وبالتالي فمن الصعب اكتشاف هذا النوع من الرقابة أو التحايل عليه.

مستويات الرقابة الإلكترونية؟

١- الرقابة المنزلية:

لا يستطيع الآباء في ظل هذا التطور التكنولوجي مراقبة ما يشاهده أبناءهم على شبكة الانترنت أو التحكم فيه، ولذلك يلجأ معظم الآباء إلى وسائل رقابية لمنع وفلترة بعض المواقع التي تضمن محتوى عنيف أو إباحي أو مؤذي لأطفالهم، ويتم ذلك باستخدام تقنية القائمة السوداء أو بالحجب من خلال كلمات البحث أو باستخدام جدار ناري لمنع وصول أبناءهم إلى بعض المواقع.

٢- الرقابة على مستوى الشركات ونطاقات العمل:

تقوم كثير من الشركات بحجب بعض المواقع عن موظفيها لضمان زيادة الإنتاجية وعدم استخدام الشبكة في غير نطاق العمل، فتستخدم أساليب الرقابة الإلكترونية والحجب والمنع سواء بكلمات البحث أو باستخدام جدار ناري.

٣- الرقابة على المستوى الدولي والحكومات:

هناك قوانين في جميع الدول تحدد نوعية المعلومات والمواقع التي تسمح لمواطنيها ومؤسساتها بالولوج إليها، وتتدرج رقابة الدول بدءا من منع أو فلترة بعض المواقع أو كلمات البحث وحتى الوصول إلى منع استخدام الانترنت بشكل كامل.

وتفعل الدول ذلك إما لأسباب اجتماعية، مثل مواقع الجنس والمقامرات وأي مواقع ترى الدولة تضمنها لمواد ضارة أو عدوانية أو مؤذية للسلوك الاجتماعي لمواطنيها.

وقد تكون أسباب سياسية، مثل حجب مواقع معارضة لسياسة الدولة أو تتضمن مواد لا توافق الدولة على تداولها أو تهتم بالحريات وحقوق الإنسان في دول بها أنظمة متسلطة وديكتاتورية.

أو لأسباب أمنية، مثل كل المواقع التي تتضمن تقنيات مراوغة أو هروب من رقابة الدولة على الإنترنت أو أي مواقع لها علاقة بصراعات أو حروب أو إحداث عنف أو أزمات.

أزاي بتحصل الرقابة الإلكترونية؟

لفهم كيفية حدوث رقابة إلكترونية، لابد من فهم آلية عمل الأنترنت وكيفية الوصول لموقع على الانترنت.

عندما تتصفحون الانترنت في المنزل أو مقهى عام، فأنتم تتصلون بالشبكة العنكبوتية بواسطة أحد مزودي خدمة الانترنت الذي يقوم بإعطاء الحاسوب الذي تستخدمونه عنواناً (عنوان IP أو عنوان بروتوكول الانترنت) ويشبه إلى حد ما العناوين البريدية في أنه يستخدم لتعريفكم وتبادل المعلومات معكم، ويكون بإمكان أي شخص يعرف عنوان بروتوكول الانترنت الخاص بكم أن يتوصل إلى مكانكم الجغرافي.

والأمر كذلك بالنسبة إلى مواقع الانترنت، فهي أيضاً لها عناوين IP؛ وفي واقع الامر، فأنتم تقومون بطلب المعلومات من عنوان آي بي معين في كل مرة تستعرضون فيها صفحة ما على حاسوبكم. وبسبب صعوبة تذكر هذه العناوين، فإن نظام مخدمات أسماء النطاقات يعطيها أسماء يمكن لنا قراءتها وتذكرها هي "أسماء النطاقات"، مثل (www.google.com)، أي أن نظام أسماء النطاقات يعمل وكأنه دليل هاتف ضخم يربط بين الأسماء وأرقامها.

ويعني هذا أنّ سلسة من الأشياء تحدث عندما تطلبون من متصفحكم فتح موقع مثل "فيسبوك" إذ يقوم حاسوبكم بطلب عنوان الآي بي الخاص بهذه الصفحة من أحد مخدمات أسماء النطاقات الكثيرة، وعادة ما يكون هذا المخدم تحت إدارة مزود خدمة الانترنت، ويطلب متصفحكم من مزود الخدمة هذا أن يتصل بعنوان الآي بي المطلوب.

بعد ذلك، يمر الطلب عبر سلسلة من الموجهات وهي نقاط اتصال يرسل كل منها نسخة من الطلب إلى الموجه التالي الأقرب للهدف، حتى يصل الطلب إلى موجه متصل بالحاسوب الذي يحوي على الموقع الذي تريدون فتحه. في نهاية

المطاف، يتم إرسال الموقع المطلوب إليكم وعرضه على شاشتكم. طبعاً لا تستغرق جميع هذه الخطوات أكثر من أجزاء من الثانية.

وليكون بمقدور مزودي خدمة الانترنت إرسال حزمة من المعلومات من حاسوب إلى موجه ومن ثم إلى حاسوب آخر، لا بد لهذه المزودات من أن تتبع قوانين دولية معينة.

تسمح هذه القوانين، والتي تعرف أيضاً بالبروتوكولات، بمشاركة البيانات والموارد على نحو منظم. فعلى سبيل المثال، تستخدم الانترنت منافذ مرقّمة لتوزيع الاتصالات على مجموعات مختلفة من الطلبات، فيتم تصفح شبكة الانترنت المعتاد عبر المنفذ رقم ٨٠ في حين يجري إرسال الملفات عبر المنفذ رقم ٢١، ويستخدم البريد الإلكتروني المنافذ ٢٥ أو ٥٣ أو ١٤٣، وتستخدم الاتصالات الهاتفية المنفذ رقم ٥٠٦٠، وذلك لأن الشبكة جزء فقط من الانترنت.

هذا وتستخدم أدوات التحايل على الرقابة المنافذ المرقمة ذاتها، فيستخدم بروتوكول القشرة الآمنة المنفذ رقم ٢٢ وتستخدم الشبكة الافتراضية الخاصة (VPN)المنفذ رقم ١٧٢٣.

وبناء على هذه القوانين، تتصل السلطات المسؤولة عن الانترنت في كل بلد ببقية العالم من خلال موجهات ضخمة، ويمكن أن تصبح هذه الاتصالات مع العالم الخارجي نقاطاً يمكن من خلالها مراقبة حركة انتقال المعلومات عبر الانترنت أو السيطرة عليها على مستوى الدولة.

تتم الرقابة الاحترافية على مستوى الحكومات ومزودي خدمة الانترنت من خلال أجهزة متطورة تكنولوجياً يمكنها أن تمسح عناوين الأي بي أو عناوين المواقع بسرعة هائلة. ورغم أن الرقابة على الانترنت شائعة في دول الشرق الاوسط، فعادة ما تأتي تكنولوجيا الرقابة من الدول الغربية الليبرالية. ومن الشركات الأشهر في مجال إنتاج الأجهزة والبرامج التي تستخدم في الرقابة على الانترنت: Cisco، وWebsense، وMcAfee، وتتمتع هذه الشركة الأخيرة بشهرة إضافية كونها الشركة التي طورت برنامج مكافحة الفيروسات المعروف.

كما ظهرت شركة Blue Coat systems، وهي أيضاً شركة تنتج معدات تستخدم في الرقابة على الانترنت ويقع مركزها في كاليفورنيا، والتي يعمل معها عدد من الأنظمة السلطوية في الشرق الأوسط وأجهزتها الأمنية ومنهم مصر.

إيه هي أشهر أساليب مراقبة الانترنت؟

١- إلغاء تسجيل بنود من مخدمات أسماء النطاقات:
وهو ما يحدث عندما تقوم السلطات في الدول التي تسيطر فيها حكوماتها على مخدمات أسماء النطاقات بإلغاء تسجيل" المواقع المحظورة. ويشبه هذا الإجراء حذف اسم شخص ما من دليل الهاتف أو كتابة رقم غير صحيح إلى جانب الاسم.

٢- حجب عناوين الآي بي:
وهو ما يحدث عندما تكون نقاط الاتصال (الموجهات) التي يستخدمها مزود خدمة الانترنت تحت سيطرة السلطات. ببساطة، تقوم هذه السلطات ببرمجة نقاط الاتصال بحيث تحجب عناوين الآي بي لمجموعة معينة من المواقع والمحتويات التي ترغب السلطات بحجبها، فيقطع مزود خدمة الانترنت الاتصال إن حاولتم الوصول إلى أحد هذه المواقع المحظورة ويظهر لكم متصفحكم رسالةَ تقول بوقوع خلل ما.

٣- الحجب على أساس كلمات البحث:
وهو ما يحدث عندما تريد السلطات حجب محتوى معين مثل المواقع التي تحتوي على كلمة "إسرائيل" أو "معارضة"، وذلك لأن حجب عناوين الآي بي وإلغاء تسجيل بنود من مخدمات أسماء النطاقات لا يحجبان إلا المواقع الموجودة بالأصل على قائمة الحظر.

وهناك الكثير من الطرق لمسح محتوى موقع ما بغرض الرقابة، إلا أن ارتفاع تكلفة مسح كل موقع بعينه، وحجم الوقت الذي يتطلبه مثل هذا العمل، يجعل معظم مزودي خدمة الانترنت يلجؤون إلى مسح عناوين المواقع عوضاً عن مسح المواقع ذاتها.

٤- تصفية الحزم:
تعدّ تصفية الحزم أكثر طرق حجب المعلومات تطوراً، وللقيام بهذا، يحتاج مزود خدمة الانترنت إلى تنصيب معدات خاصة تقرأ وتفتح جميع البيانات التي يرسلها أو يستقبلها مستخدم ما. وتدعى هذه الطريقة بتصفية الحزم لأن تبادل البيانات عبر الانترنت يتم من خلال ما يسمى "بالحزم". وإحدى الطرق الشائعة لمنع مزود خدمة الانترنت الذي تتعاملون معه من مسح بياناتكم هو تشفيرها، إذ لا يستطيع المزود تفحص ما داخل الحزم التي ترسلونها أو تستقبلونها بعد أن يتم تشفيرها. ولكن ولسوء الحظ، فإن بعض مزودي خدمة الانترنت أصبحوا الآن يحجبون الحزم المشفرة.

٥- حجب المنافذ:

يعد حجب منافذ معينة طريقة أخرى شائعة لحجب المعلومات، حيث يستخدم الانترنت منافذ معينة محجوزة مسبقاً لأنشطة بعينها، وبالتالي فإن حجب منفذ معين يؤدي بسهولة إلى منع حركة المعلومات عبر الاتصالات الهاتفية، منع عمل بعض أدوات التحايل على الرقابة، أو منع خدمات إرسال الملفات أو البريد الإلكتروني.

٦- حذف نتائج البحث:

عادة ما تتعاون المنظمات التي تبدو وكأنها تعارض الرقابة، مثل جوجل، وياهو، وبلاك بيري، وآبل، ومايكروسوفت مع الحكومات لحجب البيانات عن مستخدمي الانترنت أو مراقبتها أو تسجيلها. وفي حين يدعي موقع جوجل الشفافية حول هذا التعاون، لكونه ينشر تقريراً سنوياً عن الشفافية يصرح فيه عمّا يحجبه، فلا تتمتع جميع المواقع بهذا المستوى من الشفافية. كما يجب أن يدرك مستخدمو الانترنت أنّه عادة ما تتعاون كبرى شركات تكنولوجيا المعلومات مع حكوماتها.

٧- حجب أجزاء من الانترنت:

يعد حجب جميع أشكال الاتصال بالإنترنت شكل متطرف من الرقابة. ولكن، وبما أنّ الحكومات تملك البنية التحتية للإنترنت أو تتحكم بها في معظم دول الشرق الأوسط، فبإمكان هذه الحكومات إغلاق الانترنت عندما ترى لذلك ضرورة.

فعلى سبيل المثال، تم إغلاق الانترنت لمدة أسبوع خلال ثورة ٢٥ يناير وقامت الحكومة السورية بشيء من هذا القبيل بعد ذلك. ومع ذلك يبقى من غير الوارد حدوث هذا النوع من الرقابة كثيراً وذلك بسبب الآثار المالية الهائلة التي تنتج عن إغلاق الانترنت.

٨- وسائل أخرى للرقابة:

توجد وسائل أخرى عديدة لممارسة الرقابة على محتوى الانترنت، وعادة ما يكون لشركات الانترنت سياساتها الخاصة لمراقبة المحتوى، كما هو الحال، على سبيل المثال، في موقع فيس بوك، الذي يفرض رقابة نشطة على مستخدميه فيما يتعلق بالعري، والعبارات العدائية والعنصرية، والتمييز. وطبعاً يكمن الخطر هنا في أن فيس بوك نفسه هو من يقرر طبيعة المواد التي تقع ضمن هذه الفئات الممنوعة.

ولأن الحجب يبدو عادة وكأنه خلل تقني أو مشكلة في الاتصال، فمن الصعب معرفة ما إن كنتم تتعرضون بالفعل للرقابة وتحديد التقنية المستخدمة لمراقبة نشاطكم.

كما أنه لا يكون من الواضح عادةً من هو المسؤول عن هذه الرقابة: الحكومة، أم مزود خدمة الانترنت، أم المخدم المحلي مثل مدرستكم أو مقهى الانترنت الذي تستخدمونه، مما يجعل من الصعب التحايل على هذه الرقابة دون إجراء بحث دقيق وتفصيلي لتحديد المشكلة والحل المطلوب لمواجهتها، وعلاوة على ذلك، لا توجد حلول عامة تنفع في جميع الحالات.

أكثر الدول تشددا في الرقابة على الإنترنت؟

حسب إحصائية قامت بها "مراسلين بلا حدود"، عام ٢٠٠٦، تم تصنيف الدول الأكثر تشددا في الرقابة الإلكترونية كالآتي:

١- روسيا البيضاء
٢- بورما
٣- الصين
٤- كوبا
٥- مصر
٦- إيران
٧- كوريا الشمالية
٨- السعودية
٩- سوريا
١٠- تونس
١١- تركمانستان
١٢- أوزبكستان
١٣- فيتنام

ماذا عن الرقابة الإلكترونية في مصر؟

في مقال كتبه "أحمد عزت" على موقع "مدى مصر" يتناول فيه تطور مستوى الرقابة الإلكترونية في مصر، وضح فيه عدم اكتفاء الحكومة المصرية بالطرق التقليدية للرقابة التي تفرضها على الإنترنت خصوصا والاتصالات بوجه عام. وكيف تمحورت تلك الرقابة لسنوات حول الملاحقات القضائية للمستخدمين بدعاوى مختلفة، وتحاول الحكومة تطويرها اليوم لتنتقل إلى مرحلة المراقبة الشاملة للنشاط الرقمي للمستخدمين، ليس فقط ما يتعلق بالمحتوى العام، بل أيضاً محادثات ومراسلات الأفراد التي تتم عبر بعض التطبيقات الرقمية مثل "فايبر" و"واتس آب".

وفي إطار تطوير استراتيجية النظام المصري من مستوى الرقابة المحدودة إلى المراقبة الشاملة لأنشطة مستخدمي مواقع التواصل الاجتماعي ومحادثاتهم ومراسلاتهم الشخصية، أعلنت الحكومة ممثلة في وزارة الداخلية عن إجراء مناقصة بطريقة الممارسة المحدودة بهدف توريد وتشغيل برمجيات تهدف إلى مراقبة النشاط الرقمي على شبكة الإنترنت.

جاء المشروع الذي أعلنت عنه الوزارة تحت عنوان "مشروع رصد المخاطر الأمنية لشبكات التواصل الاجتماعي- منظومة قياس الرأي العام" والذي أعلن عنه بتاريخ ٢٠١٤/٦/١من خلال تقرير نشرته صحيفة الوطن المصرية.

ولم تنكر وزارة الداخلية ما نشرته الصحيفة، بل أكد أحد قيادتها في اتصال هاتفي مع إحدى القنوات التليفزيونية صحة الخبر المنشور، على الرغم من دفاعه المستميت عن عدم مساس هذا المشروع بخصوصيات الأفراد أو حقهم في المعرفة أو التعبير.

وبالتأكيد أثارت هذه المعلومات غضب وقلق النشطاء المصريين خاصة مع تزامن الإعلان عن هذا المشروع مع انتهاء الانتخابات الرئاسية في مصر، وقبل الإعلان رسميا عن نتيجتها، وجاء رد الفعل من جانب النشطاء ساخراً كالعادة بإنشاء "هاشتاج" على موقعي تويتر وفيسبوك بعنوان "إحنا متراقبين".

تلا ذلك قرار بعض النشطاء والمنظمات الحقوقية مقاضاة وزارة الداخلية على إثر هذا الإعلان بأن أقاموا الدعوى القضائية رقم ٦٣٠٥٥ لسنة ٦٨ قضائية أمام محكمة القضاء الإداري.

بعد ذلك نشرت بعض الصحف أن وزارة الداخلية تعاقدت بالفعل مع شركة "مصر للنظم الهندسية" التي قيل إنها فازت بالمناقصة وهي شركة تابعة لشركة أمريكية تسمى Blue Coat متخصصة في تكنولوجيا المراقبة والتجسس، وقد كان للشركة المصرية سابقة في التعامل مع جهاز أمن الدولة المصري. وقد أدى تداول الصحف لهذه الأخبار أن قامت الشركة بحجب موقعها على الانترنت مؤقتاً. من ناحية أخرى نشرت صحف أخرى على لسان مسؤولين بوزارة الداخلية توقيع هذا التعاقد.

كشف حكم محكمة القضاء الإداري الصادر عام ٢٠١١ في قضية قطع الاتصالات خلال أحداث ثورة ٢٥ يناير أن تلك لم تكن المرة الأولى لتخطي حدود الرقابة الإلكترونية إلى المراقبة الشاملة حيث أوضح أن هناك محاولات للمراقبة بدأت وفقاً لأقل التقديرات عام ٢٠٠٨ عندما قامت وزارات الداخلية والاتصالات والإعلام بمشاركة شركات المحمول بإجراء بعض تجارب المراقبة كانت إحداها في ٦ أبريل عام ٢٠٠٨

والأخرى في ١٠ أكتوبر ٢٠١٠ وقد استهدفت التجربتين قطع الاتصالات عن مصر وكيفية حجب بعض المواقع الرقمية، وأسلوب منع الدخول على شبكة الإنترنت "لمدينة أو لمحافظة أو لعدة محافظات"، وكذلك إبطاء مواقع رقمية محددة، ووضع خطة لسرعة الحصول على بيانات مستخدمي الشبكة عقب استخدامها خلال فترة لا تقل عن ثلاثة أشهر.

كما أصدرت ذات المحكمة حكماً في عام ٢٠١٠ بصدد مراقبة خدمة رسائل المحمول المجمعة "BULK SMS"، حيث قضت بوقف تنفيذ قرار الجهاز القومي لتنظيم الاتصالات بإخضاع خدمة الرسائل النصية القصيرة المجمعة للرقابة المسبقة أو اللاحقة، وبحظر تعليق مباشرة الشركات المرخص لها لنشاطها المتعلق بتقديم تلك الخدمة على وجوب الحصول على موافقات مسبقة قبل تقديم الخدمة تقوم على (رقابة محتوى الرسائل) محل الترخيص من أية جهات.

كذلك كشفت بعض الوثائق التي تم تسريبها من داخل مقرات مباحث أمن الدولة التي تم اقتحامها من قبل بعض المواطنين في أعقاب اندلاع ثورة يناير عن محاولات للحكومة المصرية لشراء تقنيات تمكنها من التجسس على بيانات وأنشطة مستخدمي وسائل الاتصال الرقمية، وذلك من إحدى الشركات المتخصصة في صناعة هذه البرمجيات والتي تسمى "مجموعة جاما الدولية".

وباستثناء الحالات السابقة فقد اقتصرت محاولات السلطات المصرية للسيطرة على الفضاء الرقمي خلال حقبة ما قبل عام ٢٠٠٨ وحتى الآن على مطاردة النشطاء قضائيا.

كانت هذه الملاحقات تتم بمناسبة استخدام النشطاء شبكات التواصل الاجتماعي. مثل المدونات وتويتر وفيسبوك وغيرها. واعتمدت أغلبها على نصوص قانونية متفرقة في قانون العقوبات المصري، وفي قوانين عقابية أخرى صممت خصيصاً لمواجهة ما يسمى "جرائم النشر". وعلى الرغم من عدم النص صراحة على تضمين وسائل النشر الرقمية ضمن وسائل النشر المنصوص عليها في هذه القوانين العقابية، إلا أن الأخيرة كانت من المطاطية بمكان لتسمح بوقوع النشر الرقمي تحت طائلة القانون.

ملاحقة النشطاء في مصر أحد محاولات السيطرة على الفضاء الرقمي

تم الحكم في فبراير ٢٠٠٧ على المدون كريم عامر بالحبس لمدة أربعة سنوات بتهمتي ازدراء الأديان وإهانة رئيس الجمهورية بسبب محتوى قام بنشره على مدونته الشخصية رأت جامعة الأزهر الذي كان "كريم" طالباً بها آنذاك أنه مخالف للقانون.

وفي غضون عام ٢٠١٠ تم الحكم على مستخدم موقع "فيسبوك" أحمد حسن بسيوني بالحبس لمدة ستة أشهر بسبب قيامه بإنشاء صفحة على الموقع بهدف تقديم معلومات عامة للمتقدمين للتجنيد، حيث قضى "بسيوني" فترة تجنيده في الإدارة العامة للتعبئة والتجنيد، وبعد انتهاء تلك الفترة قرر أن يشارك ما لديه من معلومات عامة ومنشورة على كثير من المواقع، مع المتقدمين للتجنيد، تضمنت تلك المعلومات الأوراق المطلوبة، ومواعيد التقدم لمكاتب التجنيد، والآثار المترتبة على التخلف عن التقدم في المواعيد المحددة، وأسباب التأجيل والاعفاء وغيرها من المعلومات، وعلى الرغم من أن كافة المعلومات التي قام بسيوني بنشرها، كانت منشورة بالفعل على الكثير من المواقع ومنها موقع الهيئة العامة للاستعلامات الحكومي، إلا أن المحكمة العسكرية اعتبرت هذا المحتوى من الأسرار العسكرية التي لا يجوز نشرها إلا بإذن كتابي من وزير الدفاع حتى لو كان قد سبق نشرها.

لم تكن الرقابة على المحتوى سمة مميزة لما قبل ثورة يناير فقط، بل شهدت حقبة ما بعد يناير عدد من الملاحقات القضائية لنشطاء بسبب محتوى تم نشره على بعض مواقع التواصل الاجتماعي، حيث تم الحكم على المدون "ألبير صابر" بالحبس لمدة ثلاث سنوات في ديسمبر ٢٠١٢ بسبب عدد من المقاطع المرئية والمحتويات المكتوبة المنشورة على موقعي يوتيوب وفيسبوك بالإضافة إلى مدونته الشخصية والتي عبر من خلالها عن رأيه في بعض المسائل الدينية التي رأى القضاء المصري أنها تشكل إهانة لبعض الثوابت.

وأثناء التحقيق في قضية ألبير صابر طلبت النيابة العامة من لجنة فنية تابعة لوزارة الداخلية الدخول على مواقع التواصل الاجتماعي التي له حسابات بها، وفحص المضبوطات الرقمية التي تم العثور عليها أثناء تفتيش منزله، وقد انتهى التقرير الفني إلى أنه من خلال فحص الرسائل الخاصة بحسابه على موقع فيسبوك، تبين وجود رسائل متبادلة بينه وأصدقائه تفيد في مضمونها أنه له حساب آخر على فيسبوك غير الحساب محل الفحص، وكذا ما يفيد أنه أحد القائمين على إدارة صفحة تسمى (صفحة الملحدين المصريين)، فضلا عن وجود (رسائل) متبادلة بينه وأصدقائه تتضمن عبارات ازدراء للدين الإسلامي.

هنا تجاوزت السلطات مرحلة (الرقابة) على المحتوى الذي طرح أمامها بمناسبة التحقيق في هذه القضية إلى مرحلة "المراقبة" والبحث واقتفاء الأثر لمجمل النشاط الرقمي لهذا الناشط المتهم، بهدف إضافة اتهامات جديدة وإثبات الاتهام الأولي ضده.

بالرغم من أن هذه الملاحقات قد اتسعت لتشمل التعقيب على أحكام القضاء والدعوة للتظاهر دون تصريح من الجهات المختصة، إلا أنها لم تحد من قدرة النشطاء خلال السنوات العشر الأخيرة على استخدام الفضاء الرقمي في تبادل الآراء، بما يتضمنه ذلك الآراء الصادمة وغير المألوفة، ونشر المعرفة وتلقيها، بل والدعوة لتنظيم الفاعليات السياسية التي شكلت تحدياً حقيقياً للسلطة خاصة خلال عامي ٢٠١١ و٢٠١٢، وهو ما دفع السلطات المصرية لإعادة التفكير في استراتيجيتها، وذلك بالبحث عن بديل للرقابة التقليدية المتمثلة في تجريم محتوى معين في حالة الزج بصاحبه في تحقيق أو محاكمة جنائية، تلك الاستراتيجية يبدو أنها لم تعد تجدي نفعاً في تحقيق أغراض الجهات الأمنية في حصار المجالين العام والسياسي، وهو ما دفعها للإعلان عن مشروع "رصد المخاطر الأمنية لشبكات التواصل الاجتماعي" أو "منظومة قياس الرأي العام" وهي الاستراتيجية التي تعتمد منهج المراقبة الشاملة والمستديمة للنشاط الرقمي، عوضا عن التدخل فقط في حالة وقوع فعل يجرمه القانون أو طلب سلطات التحقيق القضائية من الجهات الأمنية التحري بشأنه.

ووفقاً لما ورد في كراسة الشروط الخاصة بالممارسة المحدودة التي أعلنت عنها الوزارة فإن الغرض من التقنيات المطلوبة هو إنشاء نظام يستطيع إجراء التحريات على مجمل النشاط الرقمي بشكل دائم، ودون ارتباط ذلك بوجود شبهات حول استخدام الفضاء الرقمي في ارتكاب أفعال مخالفة للقانون من عدمه، وذلك على عكس ما هو ثابت بالتشريعات المصرية بشأن ضوابط التحري أو الاستدلال حول أي نشاط إجرامي، أو فعل مؤثم بموجب القوانين العقابية، حيث حدد قانون الإجراءات الجنائية المصري في المادة ٢١ منه حدود سلطات مأمور الضبط القضائي، بالبحث عن الجرائم ومرتكبيها وجمع الاستدلالات اللازمة للتحقيق أو الدعوى.

هذا يعني أن سلطة مأمور الضبط القضائي في البحث والاستدلال مقيدة بوجود معلومات حول وقوع جريمة معينة، بواسطة أحد الأشخاص، أو بعضهم، وقد فصل القانون في المواد اللاحقة على هذه المادة كيفية اتصال من لهم صفة الضبط القضائي بعملية التحري وجمع الاستدلالات ذاتها، وذلك من خلال عدة وسائل، منها الحصول على الإيضاحات وإجراء المعاينات التي تسهل التحقيق في الوقائع التي تبلغ إليهم بشأن ارتكاب الجرائم، أو القبض على متهم متلبساً بارتكاب جناية أو جنحة معاقب عليها بالحبس لمدة تزيد عن ثلاثة أشهر، أو

استصدار اذن من النيابة العامة بالقبض عليه في حال انتفاء حالة التلبس، وهو ما يمتد أيضاً وفقاً للقانون ليشمل تفتيش الأشخاص والمساكن، حيث أجاز القانون لمأموري الضبط القضائي تفتيش أي شخص فقط في حالة جواز القبض عليه، وقد قضت المحكمة الدستورية العليا بتاريخ ١٩٨٤/٦/٢ في القضية رقم ٥ لسنة ٤ قضائية بعدم دستورية نص المادة ٤٧ من قانون الإجراءات الجنائية التي كانت تبيح لمأمور الضبط القضائي في حالة التلبس بجناية أو جنحة تفتيش منزل المتهم، وضبط الأشياء والأوراق التي تفيد في كشف الحقيقة إذا اتضح له من أمارات قوية أنها موجودة فيه. حيث رأت المحكمة أن عبارة "أمارات قوية" يمكن التوسع في تفسيرها، وهو ما سوف يترتب عليه التعسف في استخدام سلطة التفتيش، ومن ثم يؤدي لانتهاك حرمة الحياة الخاصة للأفراد.

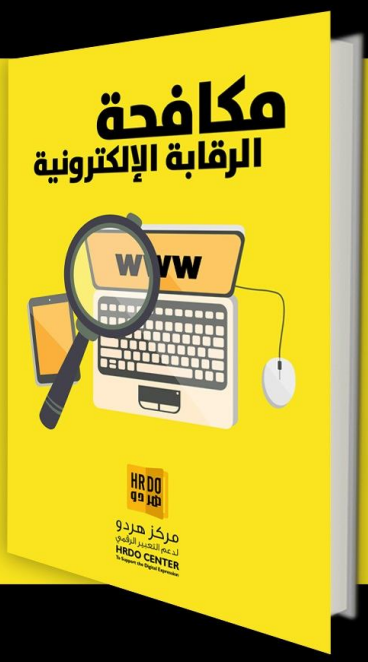
كذلك حظر قانون الإجراءات الجنائية بموجب المادة ٥٠ التفتيش إلا للبحث عن الأشياء الخاصة بالجريمة الجاري جمع الاستدلالات أو حصول التحقيق بشأنها. وعلى الرغم من أن هذه المادة أعطت استثناء للقائم بالتفتيش في ضبط أشياء أخرى غير متعلقة بالأشياء التي تطلب منه النيابة العامة التفتيش عنها إلا أن هذا الاستثناء مقيد بأن يظهر عرضا أثناء التفتيش وجود أشياء تعد حيازتها جريمة، أو تفيد في كشف الحقيقة في جريمة أخرى.

هذه المنظومة المعلوماتية التي اعتمدها المشرع المصري للبحث عن الحقيقة فيما يتعلق بالجرائم ومرتكبيها تسعى وزارة الداخلية لتطبيقها على النشاط الرقمي بصوره المختلفة لكن بشكل أشمل، مع التحرر من كافة الضوابط التي حددتها القوانين لحماية خصوصية الأفراد وحقهم في التعبير وتداول المعلومات.

فعلى خلاف الشكل التقليدي للتحريات التي ترتبط بوجود شبهات حول ارتكاب جريمة من قبل أحد أو بعض الأشخاص، فإن نظام المراقبة الذي أعلنت عنه الداخلية يسعى لجمع المعلومات والتجسس على بيانات وأنشطة مستخدمي الانترنت بصرف النظر عن وقوع أحد المستخدمين في دائرة الاشتباه من عدمه، كما أن المراقبة سوف تكون دائمة لا ترتبط بوقت محدد، فضلا عن إجرائها دون إذن قضائي، وسواء كانت هناك ضرورة للقيام بها أم لا.

مراجع

١- الشبكة العراقية للإعلام المجتمعي أنسم، "ما هي الرقابة على الانترنت؟".
https://goo.gl/0wj1Rv
٢- مقال "الرقابة على الإنترنت"، محمد اسماعيل محمد، موقع كتب.
http://goo.gl/afaCPw
٣- ويكيبيديا الموسوعة الحرة، الرقابة على الإنترنت.
https://goo.gl/EBZMMK
٤- ما الجديد في الرقابة على الإنترنت في مصر؟، أحمد عزت، مدى مصر.
http://goo.gl/mw4fX8



مكافحة الرقابة الإلكترونية

تمثل الرقابة على الانترنت وملاحقة مستخدمي التواصل الاجتماعي جزء أساسي من السلطة الأبوية التي تمارسها السلطات المصرية على المواطنين، حيث تتحكم الحكومة بهذا الأسلوب في ما يصل إلى الشعب من معلومات وأخبار وما يقومون بنشره وتداوله حسب ما يتوافق مع سياسة الدولة ونظام الحكم.

بالتزامن مع اليوم العالمي لمكافحة الرقابة الالكترونية يقدم مركز هردو لدعم التعبير الرقمي ورقة تعريفية عن اليوم، والذي تم الاحتفال به لأول مرة في ١٢ مارس ٢٠٠٨ بناء على طلب من منظمة مراسلون بلا حدود ومنظمة العفو الدولية.

تعرض الورقة في البداية تعريفا للرقابة الالكترونية والتي يقصد بها التحكم في نشر والوصول إلى المعلومات على الانترنت، وتنقسم إلى نوعين هما الرقابة النشطة التي تتم من قبل السلطات والرقابة الذاتية من قبل المواقع الالكترونية نفسها التي تتجنب الصدام مع الحكومات فتمتنع عن تقديم ما يتعارض مع النظام الحاكم.

وتوضح الورقة مستويات الرقابة الالكترونية بداية من الرقابة المنزلية للآباء على أبنائهم، والرقابة على مستوى الشركات من أصحاب الأعمال على موظفيهم، ووصولا لرقابة الدولة على مواطنيها لتحديد نوعية المعلومات التي تصل إلى المواطنين، ثم تقدم الورقة شرحا لآليات الرقابة الالكترونية وكيف تتم على المستوى التقني وكيفية التتبع عن طريق عنوان الip للمستخدم للوصول إلى موقعه الجغرافي، والقوانين التي تتحكم فيما تقدمه المواقع الالكترونية لروادها.